Form 1449 (Modified)	Atty Docket No.	RECOP017
	Application No.:	09/654,347
Information Disclosure	Inventor	Douglas B. Moran
Statement By Applicant	Group	1714
	Filing Date	August 30, 2000
(Use Several Sheets if Necessary)		

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A	5,621,889	4/15/1997	Lermuzeaux et al.	395	186	6/8/1994
	B	5,757,913	5/26/1998	Bellare et al.	380	23	4/23/1993
	C	5,844,986	12/1/1998	Davis	380	4	9/30/1996
	D	5,778,070	7/7/1998	Mattison	380	25	6/28/1996
	E	5,649,194	7/15/1997	Miller et al.	395	616	6/2/1995
	F	5,574,898	11/12/1996	Leblang et al.	395	601	1/8/1993
	G	5,724,569	3/3/1998	Andres	395	602	6/28/1995
	H	5,680,585	10/21/1997	Bruell	395	500	3/31/1995
	I	5,978,791	11/2/1999	Farber et al.	707	2	10/24/1997
	J	5,638,509	6/10/1997	Dunphy et al.	395	182.18	6/13/1996
	K						

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation Yes	Translation No
	L							

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication
	M	Rebecca Bace, INTRODUCTION TO INTRUSION DETECTION ASSESMENT, no date, for System and Network Security Management
	N	Gene H. Kim and Eugene H. Spafford, WRITING, SUPPORTING AND EVALUATING TRIPWIRE: A PUBLICALLY AVAILABLE SECURITY TOOL, March 12, 1994, Purdue Technical Report; Purdue University
	O	Douglas B. Moran et al., DERBI: DIAGNOSIS, EXPLANATION AND RECOVERY FROM BREAK-INS, no date, Artificial Intelligence Center SRI International
	P	Mabry Tyson, Ph.D., EXPLAINING AND RECOVERING FROM COMPUTER BREAK-INS, January 12, 2001, SRI International

	Q	Aleph One, SMASHING THE STACK FOR FUN AND PROFIT, no date, Volume Seven, Issue Forty-Nine; File 14 of 16 of BugTraq, r00t, and Underground.Org
	R	Donald C. Latham, DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA, December 1985, Department of Defense Standard
	S	James P. Anderson Co., COMPUTER SECURITY THREAT MONITORING AND SURVEILLANCE, February 26, 1980, Contract 79F296400
	T	Teresa F. Hunt et al., A REAL-TIME INTRUSION-DETECTION EXPERT SYSTEM (IDES), February 28, 1992, SRI International Project 6784
Examiner		Date Considered 11/29/06

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

PTO/SB/08B (08-03)

Substitute for form 1449/PTO				Complete if Known	
Information Disclosure Statement By Applicant *(Use as many sheets as necessary)*				Application No.:	09/654,347
				Filing Date	August 30, 2000
				First Named Inventor	Douglas B. Moran
				Art Unit	2136
				Examiner Name	Ronald Baum
Sheet	1	of	2	Atty Docket No.	RECOP017

U.S. Patent Documents					
Examiner Initials	Cite No.	Document Number Number-Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A.	US 6,321,338 B1	11/20/2001	Porras et al.	
	B.	US 6,484,203 B1	11/19/2002	Porras et al.	
	C.	US 6,704,874 B1	03/09/2004	Porras et al.	
	D.	US 6,708,212 B2	03/16/2004	Porras et al.	
	E.	US 6,711,615 B2	03/23/2004	Porras et al.	

FOREIGN PATENT DOCUMENTS					
Examiner Initials	Cite No.	Foreign Patent Document Country Code–Number–Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T^2
	F.	ROBERT DURST, TERRENCE CHAMPION, BRIAN WITTEN, ERIC MILLER, and LUIGI SPAGNUOLO, *Testing and evaluating computer intrusion detection systems.* July 1999 Communications of the ACM, at http://www.acm.org/pubs/contents/journals/cacm/1999-42-7/p53-durst/p53-durst.pdf	
	G.	ANDREW H. GROSS, *Analysing Computer Intrusions*, Ph.D. thesis, Electrical and Computer Engineering (Communication Theory and Systems), San Diego Supercomputer Center, University of California, San Diego, 1997.	
	H.	ROBERT W. BALDWIN, *Rule-Based Analysis of Computer Security*, Massachusetts Institute of Technology, June 1987.	
	I.	DAN ZERKLE AND KARL LEVITT, *NetKuang - A Multi-Host Configuration Vulnerability Checker*, Proceedings of the Sixth USENIX Security Symposium, San Jose, CA, July 1996.	
	J.	DAN FARMER AND EUGENE H. SPAFFORD; *The COPS Security Checker System*, Proceedings of the Summer 1990 USENIX Conference, Anaheim, CA: pp. 165-170. June 1990; Coast TR 94-01; Jun 1990. http://www.cerias.purdue.edu/homes/spaf/tech-reps/993.ps	
	K.	INTERNET SECURITY SYSTEMS; *Comparison between Internet Security Scanner (ISS) 1.x and Internet Scanner 3.2*, 1996. http://www.iss.net	
	L.	INTERNET SECURITY SYSTEMS; *Technical Specifications for Internet Scanner Version 3.0.* [This document is undated – it is believed to be 1996 or earlier based on Item F which is version 3.2 of this document.]	

Substitute for form 1449/PTO				Complete if Known	
Information Disclosure Statement By Applicant *(Use as many sheets as necessary)*				Application No.:	09/654,347
				Filing Date	August 30, 2000
				First Named Inventor	Douglas B. Moran
				Art Unit	2135
				Examiner Name	Ronald Baum
Sheet	2	of	2	Atty Docket No.	RECOP017

	M.	SAMUEL J. LEFFLER, MARSHALL KIRK MCKUSICK, MICHAEL J. KAARELS, and JOHN S. QUARTERMAN, *The Design and Implementation of the 4.3 BSD UNIX Operating System*, Addison-Wesley, 1989 Chapter 7 "The Filesystem".	
	N.	PHILLIP A. PORRAS and PETER G. NEUMANN, EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances, 1997 National Information Systems Security Conference.	
	O.	LAWRENCE HALME, TERESA LUNT, and J. VAN HORNE, *Automated Analysis of Computer System Audit Trails for Security Purposes*. Proceedings of the National Computer Security Conference, Washington, D.C., 1986.	
	P.	TERESA LUNT, *Automated Audit Trail Analysis and Intrusion Detection: A Survey*. Proceedings of the Eleventh National Computer Security Conference, Washington, D.C., October, 1988.	
	Q.	TERESA F. LUNT, ANN TAMARU, FRED GILHAM, R. JAGANNATHAN, PETER G. NEUMANN, CAVEH JALALI, *IDES: A Progress Report*. Proceedings of the Sixth Annual Computer Security Applications Conference, Tucson, AZ, December 1990.	
	R.	DAVID R. SAFFORD, DOUGLAS LEE SCHALES and DAVID K. HESS, *The TAMU Security Package: An ongoing Response to Internet Intruders in an Academic Environment*. Proceedings of the Fourth USENIX Security Symposium, October 1993, Santa Clara, CA.	
	S.	KAREN L. MYERS, *A procedural knowledge approach to task-level control*, in Proceedings of the Third International Conference on AI Planning Systems, AAAI Press, 1996.	
	T.	MICHAEL P. GEORGEFF, FRANCOIS FELIX INGRAND, *Real-Time Reasoning: The Monitoring and Control of Spacecraft Systems*, in Proceedings of the Sixth IEEE Conference on Artificial Intelligence Applications, 1990.	
	U.	MICHAEL P. GEORGEFF, FRANCOIS FELIX INGRAND, *Decision-Making in an Embedded Reasoning System*, in Proceedings of IJCAI89, Detroit, MI, 1989.	
	V.	MICHAEL P. GEORGEFF, AMY L. LANSKY, *Reactive reasoning and planning: an experiment with a mobile robot*, in Proceedings of AAAI87, 1987.	
	W.	MICHAEL P. GEORGEFF, AMY L. LANSKY, *Procedural Knowledge*, in Proceedings of the IEEE Special Issue on Knowledge Representation, Volume 74, pages 1383-1398, 1986.	
	X.	MICHAEL P. GEORGEFF, AMY L. LANSKY, *A Procedural Logic*, in Proceedings of IJCAI85, Los Angeles, CA, 1985.	

Examiner	Date Considered 11/29/06

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

T[2] = Applicant is to place a check mark here if English language Translation is attached